REMARKS

The claims and drawings have been amended to correct typographical errors and to clarify the scope of the claims. No amendments have been made for reasons relating to patentability. The Specification has been amended to expedite examination. No new matter has been introduced by way of this amendment. Full examination and favorable action are requested.

Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 09469/006001).

Respectfully submitted,

Date: 12/18/01

Richard A. Fagin, Reg. No. 39,182
ROSENTHAL & OSHA L.L.P.
1221 McKinney, Suite 2800
Houston, Texas 77010

Telephone No.: (713) 228-8600
Facsimile No.: (713) 228-8778

23590_1.DOC

Marked-Up Version of Specification

Insert before paragraph [0001]:

Cross-reference to related applications

This application claims priority from provisional application serial no. 60/246,101, filed January 25, 2001.

[0060] (Amended) Next, the PKI-Bridge (124) forwards the challenge string to the dial-up client (120) (Step 158). The dial-up client (120) forwards the challenge string to the Custom Script DLL (122) (Step 159). The Custom Script DLL (122) forwards the challenge string to the client-side cryptographic function (128) (Step 160). The client-side cryptographic function (128) uses [obtains] the dial-up user's private key on [from a] security device, and generates a signed response string (Step 161). In one embodiment of the invention, the signed response string is generated by the client-side cryptographic function (128) with the dial-up user's private key never being transferred off the security device. An example of the signed response string is described in detail below.

Marked-Up Version of Claims

[c2] (Amended) The network system of claim 1, further comprising:

a security device holding authentication information; and

a security device [card] reader attached to the client computer for reading the security device.

[c14] (Amended) A network system providing integration, comprising:

a client computer;

a server;

a server-side cryptographic function providing cryptographic services located on the server;

a PKI-Bridge providing an interface between the server and the server-side cryptographic function;

a remote access switch providing an interface between the client computer and the server;

a client-side cryptographic function providing cryptographic services located on the client computer;

a dial-up client providing dialing services to access the remote access switch;

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function;

a security device holding authentication information;

a security device [card] reader attached to the client computer for reading the security device; and

a directory service accessed by the server-side cryptographic function.

[c16] (Amended) The client computer of claim 15, further comprising:

a security device [card] reader attached to the client computer for reading a security device.

[c18] (Amended) The client computer of claim 15, wherein the custom script dynamically linked library [dial-up client] comprises a SDLogin component and a SDSetupDial component.

[c20] (Amended) A client computer comprising:

a dial-up client providing dialing services to the client computer;

a client-side cryptographic function providing cryptographic services located on the client computer;

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function; and

a security device [card] reader attached to the client computer for reading a security device.

[c24] (Amended) A method of integrating via a dial-up interface, comprising:

sending session initiation information from a dial-up client to a PKI-Bridge;

checking session initiation information by the PKI-Bridge;

generating a challenge string by a server-side cryptographic function;

forwarding the challenge string to a custom script dynamically linked library;

forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library;

utilizing [retrieving] a private key from a security device;

generating a response string;

signing the response string with the private key of a dial-in user;

forwarding a signed response string to the custom script dynamically linked library;

dividing the signed response string into packets;

forwarding packets to the PKI-Bridge;

reconstructing the signed response string from packets;

forwarding a reconstructed signed response string to the server-side cryptographic function;

obtaining a public key of the dial-in user; and

verifying the reconstructed signed response string using the server-side cryptographic function.

[c25] (Amended) The method of claim 24, further comprising:

reading the security device by a security device [card] reader.

[c34] (Amended) A method of integrating via a dial-up interface, comprising:

sending session initiation information from a dial-up client to a PKI-Bridge;

checking session initiation information by the PKI-Bridge;

generating a challenge string by a server-side cryptographic function;

forwarding the challenge string to a custom script dynamically linked library;

forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library;

utilizing [retrieving] a private key from a security device;

generating a response string;

signing the response string with the private key of a dial-in user;

forwarding a signed response string to the custom script dynamically linked library;

dividing the signed response string into packets;

forwarding packets to the PKI-Bridge;

reconstructing the signed response string from packets;

forwarding a reconstructed signed response string to the server-side cryptographic function;

obtaining a public key of the dial-in user;

verifying the reconstructed signed response string using the server-side cryptographic function;

reading the security device by a security device [card] reader;

encoding the signed response string;

decoding the signed response string;

forwarding the challenge string to the dial-up client;

forwarding the challenge string to the PKI-Bridge; and

forwarding packets from the custom script dynamically linked library.

[c35] (Amended) An apparatus of integrating via a dial-up interface, comprising:

means for sending session initiation information from a dial-up client to a PKI-Bridge;

means for checking session initiation information by the PKI-Bridge;

means for generating a challenge string by a server-side cryptographic function;

means for forwarding the challenge string to a custom script dynamically linked library;

means for forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library;

means for utilizing [retrieving] a private key from a security device;

means for generating a response string;

means for signing the response string with the private key of a dial-in user;

means for forwarding a signed response string to the custom script dynamically linked library;

means for dividing the signed response string into packets;

means for forwarding packets to the PKI-Bridge;

means for reconstructing the signed response string from packets;

means for forwarding a reconstructed signed response string to the server-side cryptographic function;

means for obtaining a public key of the dial-in user; and

means for verifying the reconstructed signed response string using the server-side cryptographic function.